

MEDIA COMMERCE SYSTEM EMPLOYING WATERMARKS

Abstract of the Disclosure

A long pseudo-random binary number, such as 128 bits, is used to represent a small increment of money (e.g., a penny, a nickel, a dime, a quarter, etc.). The long length and random character of the number essentially makes each number unique. These numbers are issued by banks or other institutions in exchange for other forms of money (e.g., cash, check, credit card, or other electronic money). The bank tracks the numbers it has issued. A consumer can transmit one or more of these numbers to a vendor to pay for goods or services. The vendor relays the numbers to a server computer (e.g., at the issuing institution, as may be indicated by a bit string appended to each binary number) to determine whether such numbers have been validly issued. If the server confirms they are valid, it informs the vendor, who then completes the transaction. The vendor's account is credited by the institution accordingly. The server marks these numbers as spent, so that if these same numbers are later presented to the server, they will not be honored as valid numbers. The long lengths of the bit strings makes hacking impractical. The system can be arranged to provide anonymity since there is no need to identify the customer in order for the merchant to redeem the tokens.